PCT - Lack of Unity Restriction

CLAIMS

1. A method for encrypting transmission traffic, comprising:

generating a variable value; and

inputting the variable value, an encryption key, and the transmission traffic into an encryption algorithm.

2. A method for transmitting authentication variables from a transmission end to a receiving end, comprising

generating a crypto-sync value at the transmission end;

generating a first authentication signature from the crypto-sync value and an encryption key at the transmission end;

transmitting the crypto-sync value and the first authentication signature to the receiving end;

generating a second authentication signature from the crypto-sync value and the encryption key at the receiving end;

incrementing the crypto-sync value at the receiving end if the first authentication signature and the second authentication signature match; and

requesting an encryption key exchange if the first authentication signature and the second authentication signature do not match.

3. The method of claim 2, wherein the step of generating the crypto-sync value at the transmission end comprises using a sequence number value, a data unit identification number, and a directional bit.

4. The method of claim 2, wherein the step of generating the crypto-sync value at the transmission end comprises using a system time value and a direction bit.

5. The method of claim 2, wherein the step of generating the first authentication signature comprises using the crypto-sync value and the encryption key in a hash function.

6. The method of claim 5, wherein the step of generating the second authentication signature comprises using the crypto-sync value and the encryption key in the hash function.

7. A method for synchronizing crypto-sync values of an encryption algorithm at a transmission end and a receiving end, the method comprising:

transmitting an encrypted message frame to the receiving end;

verifying a current crypto-sync value associated with the encrypted message frame at the receiving end;

incrementing the current crypto-sync value at the transmission end and the receiving end if the current crypto-sync value is verified; and

transmitting a failure message from the receiving end to the transmission end if the current crypto-sync value is not verified.

8. The method of claim 7, wherein the step of verifying the current crypto-sync value comprises:

decoding a plurality of transmission cyclic redundancy check (CRC) bits, wherein the transmission CRC bits are for determining transmission errors; and

decoding a plurality of encoding CRC bits, wherein the encoding CRC bits are for determining whether the current crypto-sync value generated by the receiving end matches a crypto-sync value generated by the transmission end.

9. A method for generating a message frame, comprising:

including a plurality of encoding CRC bits in a data field;

encrypting the data field, wherein a crypto-sync is used to encrypt the data field; and

appending a plurality of transmission CRC bits to the data field.

10. The method of Claim 9, further comprising:

appending sequence number information to the encrypted data field; and

appending an encryption bit to the encrypted data field, wherein the encryption bit indicates whether the data field is encrypted;

11. A system for encrypting transmission traffic, wherein the transmission traffic comprise at least two traffic types, the system comprising:

at least two encryption elements, wherein each of the at least two encryption elements is associated with at least one of the at least two traffic types; and

at least one sequence number generator for generating a plurality of sequence numbers, wherein the at least one sequence number generator is coupled to the at least two encryption elements.

12. An apparatus for independently encrypting traffic in a wireless communication system in accordance with traffic type, comprising:

a processor;

a storage element coupled to the processor comprising an instruction set executable by the processor, wherein the instruction set comprise instructions for:

generating a crypto-sync value at the transmission end;

generating a first authentication signature from the crypto-sync value and an encryption key at the transmission end;

transmitting the crypto-sync value and the first authentication signature to the receiving end;

generating a second authentication signature from the crypto-sync value and the encryption key at the receiving end;

incrementing the crypto-sync value at the receiving end if the first authentication signature and the second authentication signature match; and

requesting an encryption key exchange if the first authentication signature and the second authentication signature do not match.

13. An apparatus for independently encrypting traffic in a wireless communication system in accordance with traffic type, comprising:

a processor;

a storage element coupled to the processor comprising an instruction set executable by the processor, wherein the instruction set comprise instructions for:

transmitting an encrypted message frame to the receiving end;

verifying a current crypto-sync value associated with the encrypted message frame at the receiving end;

incrementing the current crypto-sync value at the transmission end and the receiving end if the current crypto-sync value is verified; and

transmitting a failure message from the receiving end to the transmission end if the current crypto-sync value is not verified.

14. An apparatus for transmitting authentication variables from a transmission end to a receiving end, comprising

means for generating a crypto-sync value at the transmission end;

means for generating a first authentication signature from the crypto-sync value and an encryption key at the transmission end;

means for transmitting the crypto-sync value and the first authentication signature to the receiving end;

means for generating a second authentication signature from the crypto-sync value and the encryption key at the receiving end;

means for incrementing the crypto-sync value at the receiving end if the first authentication signature and the second authentication signature match; and

requesting an encryption key exchange if the first authentication signature and the second authentication signature do not match.

15. An apparatus for synchronizing crypto-sync values of an encryption algorithm at a transmission end and a receiving end, comprising:

means for transmitting an encrypted message frame to the receiving end;

means for verifying a current crypto-sync value associated with the encrypted message frame at the receiving end;

means for incrementing the current crypto-sync value at the transmission end and the receiving end if the current crypto-sync value is verified; and

means for transmitting a failure message from the receiving end to the transmission end if the current crypto-sync value is not verified.